SYSTEM AND METHOD FOR DISTRIBUTED GROUP MANAGEMENT

ABSTRACT OF THE DISCLOSURE

A system of distributed group management for generating authentication information relating to a group to which users belong at a high speed on a client side and, at the same time, wherein a server side can verify this at a high speed. This system provides a group certificate issuing apparatus for issuing a group certificate on a client side based on original group information including the name of the group to which the users belong and a group certificate verification unit for verifying a legitimacy of the certificate transmitted from the client side in a server. Here, the group certificate issuing apparatus adds an issuance side processed value obtained by processing the information of the original group information by a cryptographic function to this original group information to obtain a group certificate, and the group certificate verification unit processes part of information included in the received certificate by an identical cryptographic function to obtain a verification side processed value and performs an authentication by confirming that the issuance side processed value and the verification side processed value coincide.